Massachusetts Center for Health Information & Analysis (CHIA)
Application for All-Payer Claims Database (APCD) Data

Applications for APCD data must meet the requirements set forth in regulation **114.5 CMR 22.00: Health Care Claims Data Release** and any Administrative Bulletins promulgated under this regulation. The regulation and bulletins are available online at http://www.mass.gov/chia/regs.

Information provided on pages 1-4 of this application will be posted on the internet for public comment.

A. APPLICANT INFORMATION	
Applicant Name:	
Title:	
Organization:	
Project Title:	
Date of Application:	
Project Objectives (240 character limit)	
Project Research Questions	1. 2. 3.

B. DATA REQUESTED

1. PUBLIC USE									
File	SINGLE USE* '08 – '09 – '10			REPEATED USE* '08 – '09 – '10			MULTIPLE USE* '08 – '09 – '10		
Medical Claims	☐	☐	☐	☐	☐	☐	☐	☐	☐
Pharmacy Claims	☐	☐	☐	☐	☐	☐	☐	☐	☐
Dental Claims	☐	☐	☐	☐	☐	☐	☐	☐	☐
Membership Eligibility	☐	☐	☐	☐	☐	☐	☐	☐	☐
Provider	☐	☐	☐	☐	☐	☐	☐	☐	☐
Product	☐	☐	☐	☐	☐	☐	☐	☐	☐

2. RESTRICTED USE									
File	SINGLE USE* '08 – '09 – '10			REPEATED USE* '08 – '09 – '10			MULTIPLE USE* '08 – '09 – '10		
Medical Claims	☐	☐	☐	☐	☐	☐	☐	☐	☐
Pharmacy Claims	☐	☐	☐	☐	☐	☐	☐	☐	☐
Dental Claims	☐	☐	☐	☐	☐	☐	☐	☐	☐
Membership Eligibility	☐	☐	☐	☐	☐	☐	☐	☐	☐
Provider	☐	☐	☐	☐	☐	☐	☐	☐	☐
Product	☐	☐	☐	☐	☐	☐	☐	☐	☐

* CHIA reserves the right to change proposed "use level" after review of this application.

Definitions:

- **Single Use**: Use of the data for a project or study.

- **Repeated Use**: Use of the data as an input to develop a report or product for sale to multiple clients or customers provided that it will NOT disclose APCD data. Examples include: development of a severity index tool, development of a reference tool used to inform multiple consulting engagements where no APCD data is disclosed.

- **Multiple Use**: Use of the data to develop a product or service that will be sold in the marketplace and will disclose APCD data. Examples include: a benchmark report produced by analyzing APCD data, a query tool to ease access to APCD data.

---

3. **Filters:** If you are requesting data elements from the Restricted Use dataset, describe any filters you are requesting to use in order to limit your request to the minimum set of records necessary to complete your project. (For example, you may only need individuals whose age is less than 21, claims for hospital services only, or only claims from small group products.)

File	Data Element(s)	Range of Values Requested
Medical Claims		
Pharmacy Claims		
Dental Claims		
Membership Eligibility		
Provider		
Product		

4. **Restricted data elements:** If you are requesting Data Elements from the Restricted Use dataset, list each restricted data element you are requesting on the attached Data Element List and explain why you need access to EACH Restricted Use data element for your project. Limit your request to the minimum data elements necessary to complete the project and be specific as to how each element relates to your proposed model/analytic plan. Add rows to this table as needed.

Restricted Data Element Name	Restricted Data Element Description	Data File (Medical, Pharmacy, Dental, Eligibility, Provider, Product)	Justification (reason this data element is necessary for your project)

C. PURPOSE AND INTENDED USE

1. Please describe the purpose of your project and how you will use the APCD.

2. Please explain why completing your project is in the public interest.

3. **Attach** a brief (1-2 pages) description of your research methodology. (This description will not be posted on the internet.)

4. Has your project received approval from your organization's Institutional Review Board (IRB)?
   - ☐ Yes, and a copy of the approval letter is attached to this application
   - ☐ No, the IRB will review the project on _____
   - ☐ No, this project is not subject to IRB review
   - ☐ No, my organization does not have an IRB

D. APPLICANT QUALIFICATIONS

1. Describe your qualifications to perform the research described or accomplish the intended use.

2. Describe the software you plan to use to analyze the data and the experience that the applicant's team members have in using that software.

3. Attach résumés or curriculum vitae of the applicant/principal investigator, key contributors, and of all individuals who will have access to the data.   (These attachments will not be posted on the internet.)

E. DATA LINKAGE AND FURTHER DATA ABSTRACTION

1. Does your project require linking the APCD to another dataset?
    YES ☐   NO ☐

2. If yes, will the APCD be linked to other patient level data or with aggregate data (e.g. Census data)?
    Patient Level Data ☐   Aggregate Data ☐

3. If yes, please identify all linkages proposed and explain the reasons(s) that the linkage is necessary to accomplish the purpose of the project.

4. If yes, specify the specific steps you will take to prevent the identification of individual patients in the linked dataset.

F. RE-RELEASE OF DATA

Applicants must obtain prior approval from CHIA to publish reports that use APCD files. Applicants must provide CHIA with a copy of any report at least 30 days prior to release to outside parties, including peer review and prepublication analysis by anyone other than the individuals named in this Application. CHIA will review the report to ensure that the publication will not permit identification of an individual patient or permit identification of a specific payment by individual payer. CHIA may prohibit release of reports that may permit identification of individual patients or specific payment by individual payer.

1. Describe your plans to publish or otherwise disclose any APCD data elements, or any data derived or extracted from such data, in any paper, report, website, statistical tabulation, or similar document.

2. Will the results of your analysis be publicly available to any interested party? Will you charge a fee for the reports or analysis? Please describe how an interested party will obtain your analysis and, if applicable, the amount of the fee.

3. Will you use the data for consulting purposes?

   YES ☐   NO ☐

4. Will you be selling standard report products using the data?

   YES ☐   NO ☐

5. Will you be selling a software product using the data?

   YES ☐   NO ☐

6. If you have answered "yes" to questions 3, 4 or 5, please (i) describe the types of products, services or studies; (ii) estimate the number and types of clients for which the data will be used and (iii) describe any rerelease of data by your clients.

G. USE OF AGENTS OR CONTRACTORS

Third-Party Vendors. Provide the following information for all agents and contractors who will work with the APCD data.

Company Name:	
Contact Person:	
Title:	
Address:	
Telephone Number:	
Fax Number:	
E-mail Address:	
Organization Website:	

1. Will the agent/contractor have access to the data at a location other than your location or in an off-site server and/or database?

   YES ☐   NO ☐

2. Describe the tasks and products assigned to this agent or contractor for this project.

3. Describe the qualifications of this agent or contractor to perform such tasks or deliver such products.

4. Describe your oversight and monitoring of the activity and actions of this agent or subcontractor.

Information provided from this page forward will NOT be posted publicly on the internet.

H. APPLICANT CONTACT INFORMATION	
Applicant Name:	
Title:	
Organization:	
Address:	
Telephone Number:	
E-mail Address:	
E-mail Addresses of ALL Co-Investigators:	

I. DATA SECURITY AND INTEGRITY

Please refer to the attachment on data safeguards at the end of this application.

Complete this section for *each location* where the data will be stored or accessed.
If you plan to use an agent/contractor that has access to the data at a location other than your location or in an off-site server and/or database, the agent/contractor should complete this section.

1. Please identify the person or organization that will be responsible for data security and provide contact information.

2. Attach a confidentiality agreement signed by **each** individual who will have access to the data.

3. If your organization has a Written Information Security Program (WISP) please attach it and refer to the appropriate sections of the WISP in your responses to the questions below. (This document will NOT be posted on the internet.)

4. Specify the security measures you will take to prevent unauthorized access to or use of data, including information on access restrictions; handling and storage of data; physical security of the data; audit policies and capabilities; and breach notification policies.

5. Describe in detail how the original data media and subsequent copies of the data will be protected; how mainframe, server or PC data files will be protected; where and how work files are protected; how the data on PCs are protected from access; and how internet enabled devices will be protected..

6. Describe you will ensure that the data cannot be accessed by portable devices.

7. If you plan to re-release data in an electronic format, specify the security measures you will take to safeguard the re-released data.

8. Describe any other relevant security and privacy protections.

J. DATA RETURN AND DESTRUCTION

Applicants are required to attest that the original released data and all copies of the data used by the applicant, applicant employees and/or applicant contractors and agent, will be destroyed upon completion of the project described in this Application. Specify the measures you will use to meet these requirements.

K. DATA DISCLOSURE AND USE ASSURANCES

In consideration of any data received, it is agreed that:

a) The applicant, his/her employees, and his/her agents or contractors shall use APCD data only for the purpose stated in the request.

b) The applicant shall limit access to the APCD data to authorized employees, agents, or contractors as are reasonably necessary to undertake the permitted data uses, and as named in the application. The applicant shall ensure that all such employees, agents, and contractors with access to the data comply with all data privacy and security protections and data use restrictions, prohibitions and protections set forth in regulation 114.5 CMR 22.03(2)(a)1 and sign a Data Confidentiality Agreement.

c) The applicant, his/her employees, and his/her agents or contractors shall not use the APCD data, alone or in combination with any other data, to identify individual patients, clinicians or payment rates, nor will the applicant, his/her employees, and his/her agents or contractors attempt to identify individual patients, clinicians, or payment rates from the data, or to contact individual patients or clinicians.

d) The applicant, his/her employees, and his/her agents or contractors shall not sell the APCD data, nor use the data for any marketing or commercial purposes unless approved by CHIA.

e) The applicant, his/her employees, and his/her agents or contractors shall retain the requested APCD data only as long as is necessary to accomplish the applicant's intended use or purpose. The applicant, his/her employees, and his/her agents or contractors shall return to CHIA or destroy, in CHIA's discretion, all such data, including any copies of the data, as soon as he/she has accomplished that purpose or use. CHIA may limit the amount of time within which an applicant may retain data.

f) The applicant, his/her employees, and his/her agents or contractors shall not reuse, manipulate, or re-aggregate APCD data for purposes other than those approved by CHIA.

g) The applicant shall immediately report to CHIA any use or disclosure of APCD data that is not consistent with this application, and shall immediately attempt to retrieve such data and take other appropriate actions to limit the consequences of the non-permitted use or disclosure.

h) The applicant, his/her employees, and his/her agents shall permit CHIA, its employees, and its designated agents to audit the applicant's compliance with the requirements of the Data Use Agreement at any time.

i) The applicant shall not publish or otherwise disclose any Restricted Data Elements, or any data derived or extracted from such data, in any paper, report, website, statistical tabulation, or similar document unless such paper, report, website, statistical tabulation, or similar document conforms to the standards for de-identification set forth under 45 CFR 165.514(a), (b)(2), and (c). The applicant shall not publish or otherwise disclose any public paper, report, website,

statistical tabulation, or similar document contain individual payment rates, report any data on ten or fewer individuals or data derived from ten or fewer claims.

j) The applicant will cite the Massachusetts Center for Health Information and Analysis as the source of the data in any studies, reports, or products in which the APCD data is used.

k) The applicant will indemnify the Massachusetts Center for Health Information and Analysis and Health Care Payers against any and all claims arising from the provision and use of any data released to the applicant including, but not limited to, any breach of patient confidentiality by the applicant or its employees, agents, or contractors. **The Committee requires all clients of the original data receiver to adhere to the confidentiality and security requirements contained in this application. Each client needs to sign and return to the data holder the confidentiality assurances prior to rerelease of any data.**

l) If the applicant prepares a report based upon APCD data, the applicant will submit a copy of the report to CHIA at least 30 days prior to releasing the report to another person or entity so that the Committee can determine whether the privacy rights of any data subject would be violated by such release and whether the project is consistent with the uses described in this Application. CHIA reserves the right to prohibit the publication of a report that violates the terms of this agreement.

CENTER FOR HEALTH INFORMATION & ANALYSIS
DATA USE AGREEMENT

The undersigned Applicant and all its authorized representatives, subcontractors, agents and employees, in consideration for the receipt of All-Payer Claims Database data, agree that they will observe the following conditions of use regarding All-Payer Claims Database files, or any data subsets derived from such files ("CHIA Information"):

1) Only authorized Recipient personnel may access the Information and the Information may only be shared with authorized personnel

2) CHIA Information may ONLY be stored within secure folders on secure, designated hardware or equipment.

3) Recipient personnel are prohibited from sharing ANY CHIA Information (personal level or confidential) to any third party, including vendors and subcontractors, without written authorization from CHIA.

Confidentiality and Security Requirements:

1) Paper versions of the CHIA Information must never be in the open sight of an employee not authorized to access the HCF information.

2) Paper versions of the CHIA Information must never be left unattended at an Employee's desk, the photocopy machine, the fax machine, etc.

3) The CHIA Information furnished to the Recipient, and any material generated there from, such as extra copies, photo impressions, computer printouts, carbon paper, notes, stenographic notes, and work papers, if no longer needed, must be destroyed on site by individuals who have been previously approved by CHIA to have access to the data. HCF Information must never be discarded whole, under any circumstance.

4) Any transmission of the data must occur over a secure and encrypted connection.

5) Information received from CHIA may never be maintained on a mobile or portable device. This prohibition applies to laptop computers, Blackberries, USB flash drives, I-pods, CD-Roms, DVD's, floppy disks or the equivalent of any of these devices. Violation of this prohibition shall be grounds for immediate termination of the data exchange agreement.

6) Recipient is not allowed to transfer the CHIA Information to any other agency or third party, including contractors, without the prior written approval of CHIA.

7) Access to areas containing the CHIA Information in any form (computer printout, photocopies, tapes, DVDs, notes, etc.) during the normal business day must be limited by creating restricted areas, security rooms, or locked rooms or files. Additionally, the CHIA Information in any form (computer printout, photocopies, tapes, notes, etc.) must be protected during non-business hours by secured or locked premises, secured areas, or containerization.

8) The CHIA Information may not, under any circumstance, be taken off of the Recipient's worksite.

9) No work involving CHIA Information will be contracted without prior written approval of CHIA. The identities and personal information of all contractors, vendors and non-agency employees will be provided to CHIA for whatever background investigation CHIA deems necessary prior to these individuals having access to the CHIA Information.

Applicable Massachusetts Legal Requirements

The undersigned hereby agrees to comply with the requirements set forth in:

1) Fair Information Practices Act (FIPA), G.L. c. 66A: Prohibits the unauthorized disclosure of "personal data," as defined in G.L. c. 66A. Data subjects may make a claim for damages under the Massachusetts Tort Claims Act. General Laws chapter 214, section 3B also provides for injunctive and other nonmonetary relief for violation of this statute.
2) Executive Order 504 – Order Regarding the Security and Confidentiality of Personal Information
3) 114.5 CMR 22.04 – Data Disclosure Restrictions

The undersigned acknowledges that failure to adhere to these requirements could result in forfeiture of data received and forfeiture of the right to receive All-Payer Claims Database data in the future, as well as other applicable statutory sanctions and 114.5 CMR 22.00.

Applicable Federal Statutes

The undersigned hereby agrees to comply with the requirements set forth in:

1) Privacy Act of 1974, 5 U.S.C. § 552a: Provides that a person who has access to records that contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act, and who willfully discloses the material to anyone not entitled to receive it, is guilty of a misdemeanor and may be fined not more than $5,000.
2) Health Insurance Portability and Accountability Act of 1996 (HIPAA)
3) Health Information Technology for Economic and Clinical Health Act (HITECH)

The undersigned acknowledges that failure to adhere to these requirements could result in forfeiture of data received and forfeiture of the right to receive All-Payer Claims Database data in the future, as well as other applicable statutory sanctions.

Signature

Name of Applicant:

Title of Applicant:

Applicant's Organization:

Date_____   _____
                                                            Signature of Applicant

CONFIDENTIALITY AGREEMENT FOR THE USE OF APCD DATA
SIGNATURE PAGE

I, _____, hereby acknowledge that, in connection with my request for All-Payer Claims Database data under an agreement (the "Agreement") with CHIA, I may acquire or have access to confidential information. This information includes, but is not limited to, patient level protected health information (PHI - eligibility, claims, providers), health insurance coverage information, financial institution match information, as well as "personal data" as defined in G.L. c. 66A (collectively, the "Information")

I will at all times maintain the confidentiality of the Information. I will not inspect or "browse" the Information for any purpose not outlined in the Agreement. I will not access, or attempt to access, my own Information for any purpose. I will not access, or attempt to access, Information relating to any individual or entity with which I have a personal or financial relationship, for any reason. This includes family members, neighbors, relatives, friends, ex-spouses, their employers, or anyone not necessary for the work assigned. I will not, either directly or indirectly, disclose or otherwise make the Information available to any unauthorized person at any time, either during or after my employment with CHIA.

I agree to comply with all laws relating to confidentiality of the Information, including but not limited to, the following:

1) Fair Information Practices Act (FIPA), G.L. c. 66A: Prohibits the unauthorized disclosure of "personal data," as defined in G.L. c. 66A. General Laws chapter 214, section 3B provides for injunctive and other nonmonetary relief for a violation of the statute.

2) G.L. c. 93H, § 3: Requires a person or an agency of the Commonwealth to provide written notification to the Attorney General, Director of Consumer Affairs and Business Regulation, Information Technology Division, Public Records Division and the affected individual when a person engages in any unauthorized access or use of an individual's personal information.

3) Privacy Act of 1974, 5 U.S.C. § 552a: Provides that a person who has access to records that contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act, and who willfully discloses the material to anyone not entitled to receive it, is guilty of a misdemeanor and may be fined not more than $5,000.

If I have access to information about myself or any member of my immediate family, I agree to self-identify to CHIA. I also acknowledge that I will be restricted from access to my or my immediate family's personal account for any purpose.

The Applicant or his/her employer must submit to CHIA an addendum listing all individuals who will have access to APCD data. Each listed individual must sign an agreement to comply with the terms of the Data Use Agreement. This addendum must be updated annually of data is requested for subsequent years (for example, requesting APCD data through 2015).

_____   _____

Authorized Signatory   Date

Print Name:_____

Title:_____

Organization:_____

Address:_____

Telephone:_____ FAX:_____

Email:_____

CERTIFICATION OF PROJECT COMPLETION & DESTRUCTION OR RETENTION OF DATA

NOTE: Data must be destroyed so that it cannot be recovered from the electronic storage media. Acceptable methods include the use of file wiping software implementing at a minimum DoD.5200.28-STD (7) disk wiping, and the degaussing of backup tapes. Electronic storage media such as floppy disks, CDs, and DVDs used to store data must be made unusable by physical destruction.

The undersigned hereby certifies that the project described in this Application is complete as of this date: _____

The undersigned further certifies as follows (check the appropriate section):

☐ I/we certify that we have destroyed all data received from CHIA in connection with this project, in all media that was used during the project. This includes, but is not limited to, data maintained on hard drives and other storage media.

☐ I/we certify that we are retaining the data received in connection with the aforementioned project pursuant to the following health or research justification (please include an attachment providing detail and state how long the data will be retained).

☐ I/we certify that we are retaining the data received from CHIA in connection with the aforementioned project as required by the following law:
[Reference the appropriate law and indicate the timeframe]

_____

SIGNATURES:

Applicant: _____

Date: _____

For the Applicant's Organization: _____

APPLICATION SUMMARY SHEET / CHECKLIST

Please complete and return this checklist along with the application. Thank you.

Data Requested:

Boxes clearly marked on Page 2?   ☐ YES   ☐ NO

If requesting Restricted Data Elements, Data Element List included?   ☐ YES   ☐ NO   ☐ N/A

Security Program Included?   ☐ YES   ☐ NO

Description of research methodology included?   ☐ YES   ☐ NO

CV/resumes of PI, key contributors, and data users included?   ☐ YES   ☐ NO

Confidentiality Agreement signed by each data user included?   ☐ YES   ☐ NO

Intended Use(s) of Data

Check *all* uses that describe your *intended use(s)* of the data requested:

☐ Clinical research   ☐ Health services research
☐ Health outcomes   ☐ Quality
☐ Medical practice patterns   ☐ Market Analysis
☐ Utilization   ☐ Access to care
☐ Cost   ☐ Other_____
☐ Analyses to address public policy issues   _____
☐ Analyses to address commercial or market-specific issues
☐ Create products and tools

Submit your completed request:
1) In a Word document AND a scanned pdf of the signed document by email to apcd.data@state.ma.us.

===
The following section is for CHIA use only:

*Date Received***:_____**

Data Use Classification: Single use: _____
                                Limited multiple uses: _____
                                Multiple uses: _____

SAFEGUARDING THE CENTER FOR HEALTH INFORMATION & ANALYSIS'S INFORMATION

I.　　Purpose

This document is to establish and maintain uniform confidentiality and security standards and procedures that must be adhered to by all Recipients of information from the MA Center for Health Information & Analysis (CHIA) to ensure that the policies, practices, controls, and safeguards employed by recipients adequately protect this confidential information. This Document is an Addendum to any data agreement between CHIA and the Recipient.

II.　　Definitions

For the purpose of this document, the term:

"Recipient" shall include any state agency or other entity receiving information from CHIA.

"Employee" shall include all state and non-state employees, contract employees, individual consultants, volunteers, trainees, student interns, members, directors, officers, partners, agents and subcontractors who may have access to the confidential information.

"CHIA Information" shall include any type of information received from CHIA, including, but not limited to, medical, pharmacy and dental claims information, eligibility/member information, patient encounter information, and any other information identified as confidential information.

"Media" shall include all forms of physical storage such as Compact Disks (CDs), DVDs, tapes, drives, and other storages devices.

III.　　General Safeguard Requirements

The Recipient must assign a Contract Manager, at a Director level or higher, to assume full responsibility for, and ensure compliance with, the Recipient's safeguard standards and procedures. The Recipient must furnish a current organizational chart to demonstrate the individual's role and function within the organization.

When a data exchange agreement expires or is terminated, all CHIA Information, files, and media in possession of the Recipient are to be destroyed or returned to CHIA. The Recipient must sign an affidavit confirming that all CHIA Information, files and media have been returned to CHIA's Health Information Team. The Health Information Team will confirm the data from all sites and facilities where it had been maintained have been cleared.

Access to areas containing the CHIA Information in any form (computer printout, photocopies, Media, notes, etc.) during the normal business day must be limited by creating restricted areas, security rooms, or locked rooms or files. Additionally, the CHIA Information in any form (computer printout,

photocopies, Media, notes, etc.) must be protected during non-business hours by secured or locked premises, secured areas, or containerization.

The Recipient will implement rules and procedures to ensure that Employees do not leave computers or paper containing the CHIA Information unprotected at any time.

The CHIA Information must never be commingled with other Recipient information without the written approval of CHIA.

The CHIA Information must never be transmitted or used on E-mail systems or sent via the Internet unless encrypted.

The CHIA Information may not, under any circumstance, be taken off of the Recipient's worksite.

IV.   **Safeguard of Paper Copies of CHIA Information Received**

The Agency shall send written notice to CHIA within 48 hours if any employee authorized to access CHIA Information has been terminated, laid off or involuntarily removed in any way from his/her employment for any reason connected to a breach or misuse of CHIA Information. This requirement also applies to contractors, vendors or temporary workers.

The Recipient will take every precaution available to ensure the physical security of the CHIA Information under its control, including, but not limited to: fire protection; protection against smoke and water damage; alarm systems; locked files or rooms; limited access; or other means to prevent loss or unauthorized removal of manually held data.

The CHIA Information must never be in the open sight of an Employee not authorized to access the CHIA Information.

The CHIA Information must never be left unattended at an Employee's desk, the photocopy machine, the fax machine, etc.

The CHIA Information furnished to the Recipient, and any material generated therefrom, such as extra copies, photo impressions, computer printouts, carbon paper, notes, stenographic notes, and work papers, if no longer needed, must be destroyed on site by individuals who have been previously approved by CHIA to have access to the data. CHIA Information must never be discarded whole, under any circumstance. The Agency must maintain a log and inventory documenting the shredding of CHIA Information.

Shredding must be conducted in conformance with applicable state and federal regulations.

V.   **Safeguard of Electronic Copies or Maintaining CHIA Information Received on Recipient or Entity Computer System**

The Recipient will continuously monitor the use of the CHIA Information maintained on its computer system to ensure that access to this system is limited to personnel with authorization and who have an approved business need for the CHIA Information.

The Recipient will require: passwords; access logs; badges; limited terminal access; limited access to input documents; design provisions to limit use of the Information; and any other method necessary to protect the data and to prevent loss or unauthorized access to the CHIA Information. Appropriate data center access control logs must be maintained by the Recipient.

The Recipient will work with the users to ensure that all passwords have certain parameters; including, but not limited to; at least eight characters with one character consisting of at least one number or special character; and a mix of upper and lower case letters. Administrative passwords must be complex and be maintained by the system administrator of the server and be unique to the functional area. No single password is to be maintained across all servers.

The Recipient will conduct periodic data purifications and user account validation. The Agency will immediately terminate access to the computer system of any person that is no longer authorized to access the CHIA Information.

Any transmission of the data must occur over a secure and encrypted connection.

The Recipient's server system must be a dedicated system on an isolated network segment with a current Antivirus running at all times and housed in a physically secure computer room with limited authorized personnel access controls in place. Only those individuals approved by CHIA to access the data will be allowed access to the CHIA Information in the system.

Information received from CHIA may never be maintained on a mobile or portable device. This prohibition applies to laptop computers, Blackberries, USB flash drives, I-pods, CD Roms, DVD's, floppy disks or the equivalent of any of these devices. Violation of this prohibition shall be grounds for immediate termination of the data exchange agreement.

The CHIA Information may be stored on hard disks only if Recipient -approved security access control devices (hardware/software) have been installed, are receiving regularly scheduled maintenance, including upgrades, and is being used. Access control should include password security, an audit trail, encryption or guided media, virus detection, and data overwriting capabilities. The CHIA Information should never be maintained on any disk not specifically authorized, in writing, by CHIA.

Magnetic tape containing the CHIA Information should be maintained in a separate pool of tapes and must not be made available for reuse or released for destruction without first being subjected to electromagnetic erasing. If reuse is not intended, the tape should be destroyed by cutting into lengths of 18 inches or less or by burning to effect complete incineration. All CHIA Information stored on magnetic media must be encrypted using either a software or hardware encryption methodology.

All transaction access to the CHIA Information must be logged and maintained for the period legally required based upon the data being accessed. The Recipient must house and maintain these logs. The

Recipient will be required to provide access to this information to state, federal and CHIA authorized contractors upon request.

The Recipient is not allowed to transfer the CHIA Information to any other agency or third party, including contractors, without the prior written approval of CHIA. All approved data transfers are subject to the same, or additional conditions as defined in the data exchange agreement.

The Recipient may maintain the CHIA Information on its system only for as long as it is relevant or useful to the Recipient. The Recipient is responsible for the data destruction upon the end of the data life or upon the termination of this data exchange agreement and must provide proof of the destruction to CHIA. The Recipient is required to follow the best practices contained in the NIST 800-53 Standard regarding the destruction of electronic or paper media.

VI.   **VENDORS**

No work involving the CHIA Information will be contracted without prior written approval of CHIA. The identities and personal information of all contractors, vendors and non-agency employees will be provided to CHIA for whatever background investigation CHIA deems necessary prior to these individuals having access to the CHIA Information.

The Recipient must account for the use of all vendors, permitted by law or regulation, to do programming, processing, or administrative services requiring access to the CHIA Information.